# ATTACHMENT A

## Remarks

Considering the matters raised in the Office Action and turning first to the rejection on prior art, claims 1-11 have been rejected under 35 USC 103(a) as being "unpatentable over Veil et al. (U.S. Patent 6,092,202) as applied to claim 1 above, and further in view of Beckert et al. (U.S. Patent 6,862,61)." This rejection is respectively traversed although claim 1 has been amended to even more clearly distinguish over the cited references.

Claim 1 has been amended to further underscore the fact that the claimed computer system controls the operation of at least one public transport vehicle and, in particular, manages the operation of at least one public transport vehicle so as to ensure safe operation thereof. Claim 1, as amended, recites that the peripheral computes a code for each elementary operation performed by the processor and verifies proper operation of all or part of the executed program controlling the processor "by detecting any errors produced in the operation of the processor" and also recites that the control system "controls the safe operation of the at least one public transport vehicle based on said detecting of internal errors as well as detecting external errors." Support for the amendments made to claim 1 is provided, inter alia, by the first three paragraphs on page 8 of the specification.

Turning to the references, the Beckert patent relates to an automatic computer device with emergency power shutdown capabilities. Power is provided to "a small amount of static RAM that is incorporated into the computing device." Software manages the static RAM and this software "knows exactly where all of the object store pages are located so that in the event of a power loss, the page locations are known and hence the pages can be used when power is restored." Hence, Beckert is exclusively concerned with securing the storage of pages when a shutdown occurs.

Veil is essentially concerned with preventing hackers from hacking into electronic transactions and, in this regard, secure processing is carried out in the security co-processor, and non-secure processing is carried out in the host computer. Hence, Veil is not concerned with errors that occur during, or are generated by or from, the

computer system itself, but is rather concerned with external errors, i.e., intrusions or false authentications, that place the computer in an unsecured state.

The present invention, as claimed in the claims as amended, is especially concerned with providing safe operation of a public transport system. It is respectively submitted that the Veil and Beckert patents relate to very different fields from that of the present invention and from each other, and it simply would not be obvious to combine the two.

In the "Response to Arguments" section, it is argued in support of the obviousness of the combination that "[i]n this case, the proposed system provides automatic computer devices for controlling the vehicles, as well as during emergency power shut down in vehicle computer, where an interface interfaces a security coprocessor to a host computer for controlling the vehicles." This argument is not understood. First, the Veil reference has nothing whatsoever to do with vehicles of any kind and the passages to which the Examiner refers relate to separately processing secure transitions in the security co-processor 122, rather than in the PC 114, which, as has been repeatedly pointed out, is the opposite of what is being claimed.

Further, the Beckert patent deals with an entirely different problem and while the patent refers to using the vehicle computer system 200 to "integrate multiple vehicle-related systems into one open platform hardware and software architecture," this general disclosure is not a proper basis for combining the references. The Beckert reference does not deal with the problems with which the present invention is concerned and, as indicated above, is directed to providing secure storage of data upon the occurrence of a shutdown. Veil is not concerned with the internal safety of the computer system but only provides security against external attacks. Again, it is respectively submitted that the proposed combination of Veil and Beckert is clearly the improper product of hindsight, given the actual teachings of the two references.

Moreover, even if the references were somehow combined, the resultant hybrid combination would not include the features now set forth in claim 1, as amended. In this regard, the references do not relate to computer systems for managing the operation of at least one public transport vehicle so as to ensure safe operation thereof and do not disclose verifying operation of all or part of an executed program controlling

a processor by detecting any internal errors produced in the operation of the processor, much less controlling safe operation of the at least one public transport vehicle based on said detecting of such internal errors as well as detecting external errors.

While claim 1 has been amended in order to expedite the prosecution, it is noted that claim 1, in its previous form, clearly defines over Veil. For example, claim 1 recites that the processor and the at least one peripheral both process all types of input data codes including any secure input data codes. This feature simply is not disclosed in the Veil reference and, in fact, is clearly contrary to the teachings of Veil.

As has been repeatedly pointed out, and as the Examiner apparently admits, the method disclosed in the Veil reference provides for processing of secure sensitive data in a coprocessor and for processing non-secure or non-sensitive data in the host computer. In the "Response to Arguments" section, the Examiner contends that the cited "prior art clearly teaches system and method for where an interface interfaces a security coprocessor to a host computer." The mere fact that there is an interface between the co-processor and the host computer does not change the basic teachings of Veil, viz., that processing of secure data takes place in the co-processor and processing of non-secure data takes place in the host computer.

Further, it is respectfully submitted that the other statements in the Office Action in support of the Examiner's position (i.e., that the "interface includes the communication protocol for restricting access by the host computer to the data transmitted through the coprocessor" and that "[s]ecure transaction processing is performed locally in the security coprocessor and non-secure transaction processing is performed in the host computer") actually support the position taken by applicant and clearly do not support the position taken by the Examiner in attempting to read the claim language on Veil. In the system of Veil, "the sensitive data is never processed by the computer 114 in the traditional computing environment 102 and it is therefore not acceptable to attack" (see column 7, lines 45-49). Thus, claim 1 defines over Veil for this further reason as well.

Further, claim 1 recites that the peripheral performs verification operations so as to check that the computer is operating properly. More particularly, as recited in claim 1, the peripheral "receives at least the data input codes" and "computes a code for each

elementary operation performed by the processor and verifies proper operation of all or part of the executed program." It is respectfully submitted that such codes differ from, and should not be confused with, cryptographic data. (In this regard, it is clear from the specification that the data processed by the present invention could be transmitted outside of the system in a non-encrypted form.) In any event, the purpose of computing a code for each elementary operation performed by the processor and verifying the operation of all or part of the computer program is not to protect the data against hackers (which is the core purpose of the Veil system) but, instead, to check the properties of the data and to derive therefrom whether the processor is operating correctly.

The parts of the Veil reference that are said to disclose these features have been carefully considered but it is respectfully submitted that the security co-processor of Veil does not compute codes within the meaning of that word as claimed in the claims but rather merely encrypts sensitive data, and, moreover, as indicated above, clearly does not verify the proper operation of the executed program controlling the processor. Further, Veil does not provide for any verification of the nature claimed, much less verification "at least partly based on the input data codes and the codes computed by the peripheral" as recited in claim 1. Thus, for these additional reasons it is respectfully submitted that claim 1, prior to amendment, patentably defined over Veil.

In summary, it is respectively submitted that amended claim 1 clearly defines over the cited references. Apart from the fact that they relate in some manner to computing systems, the two references have essentially nothing to do with each other nor with the present invention, and one of ordinary skill in the art would not be lead to combine these references without the improper benefit of hindsight. Moreover, as discussed above, no combination of the references could or would result in the present invention as claimed in the claims now presented. Accordingly, allowance of the application in its present form is respectively solicited.

**END REMARKS**